Serial No.: 09/705,998

1   LISTING OF CLAIMS

2   CLAIMS

3   What is claimed is:

4   1. (Original) A method for encrypting a plain-text message, the method comprising:

5   generating a first random number;

6   transforming said first random number into a first pseudo random number;

7   further expanding a randomness of said first random number and/or said first pseudo random
8   number into a set of pair-wise differentially-uniform pseudo random numbers;

9   dividing said plain-text message into a plurality of plain-text blocks;

10   encrypting said plain-text blocks to form a plurality of cipher-text blocks;

11   combining said plurality of plain-text blocks into at least one check sum; and

12   employing said set of pair-wise differentially-uniform pseudo random numbers, together with
13   said first random number and/or said first pseudo random number, to embed a message integrity
14   check in said cipher-text blocks.

15   2. (currently amended) A method as recited in claim 1, wherein the step of encrypting said
16   plain-text blocks includes employing the said first random number, and/or said first pseudo
17   random number, and/or said set of pair-wise differentially-uniform pseudo random numbers.

DOCKET NUMBER: YOR920000763US1   -5/34-

Serial No.: 09/705,998

1   3. (Original) A method as recited in claim 1, wherein the step of employing includes pairing said

2   first random number, and/or said first pseudo random number, and/or said set of pair-wise

3   differentially-uniform pseudo random numbers, with said plurality of cipher-text blocks; and

4   combining each pair to form a plurality of output blocks.

5   4. (Original) A method as recited in claim 3, wherein the step of combining each pair includes

6   performing an exclusive-or operation upon components of said each pair.

7   5. (Original) A method as recited in claim 1, wherein the step of encrypting includes encrypting

8   said first random number.

9   6. (Original) A method as recited in claim 1, wherein the step of encrypting includes encrypting

10   said check sum.

11   7. (Original) A method as recited in claim 1, wherein the step of combining includes obtaining

12   said check sum from an exclusive-or of said plurality of plain-text blocks.

13   8. (Original) A method as recited in Claim 1, wherein the step of transforming said random

14   number includes a non-cryptographic or linear operation.

15   9. (Original) A method as recited in Claim 1, wherein the step of transforming said random

16   number includes a cryptographic operation.

17   10. ((currently amended) A method as recited in Claim 1, wherein ~~the~~ said set of pair-wise

18   differentially-uniform numbers are set of pair-wise differentially-uniform numbers in GFp.

19   11. (Original) A method as recited in claim 2, wherein the step of employing includes:

DOCKET NUMBER: YOR920000763US1   **-6/34-**

PAGE 7/47 * RCVD AT 5/21/2004 2:13:07 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:9149453281 * DURATION (mm-ss):14-50

Serial No.: 09/705,998

1   pairing said first random number, and/or said first pseudo random number, and/or said set of

2   pair-wise differentially-uniform pseudo random numbers, with said plurality of plain-text blocks;

3   and

4   combining each pair to form a plurality of input blocks used in said step of encrypting.

5   12. (Original) A method as recited in claim 11, wherein the step of combining each pair includes

6   performing an exclusive-or operation upon components of said each pair.

7   13. (Original) A method for decrypting a cipher-text message, the method comprising:

8   dividing said cipher-text message into a plurality of cipher-text blocks;

9   decrypting said cipher-text blocks in forming a plurality of plain-text blocks;

10 transforming at least one of said plain-text blocks into a first pseudo random number;

11 further expanding at least one of said plain-text blocks and/or said first pseudo random number

12 into a set of pair-wise differentially-uniform pseudo random numbers;

13 combining said first pseudo random number, and/or said set of pair-wise differentially-uniform

14 pseudo random numbers, and/or said at least one plain-text block to form at least two check sums

15 and to form a plurality of output blocks; and

16 comparing said at least two check sums in declaring success of a message integrity check.

17 14. (Original) A method as recited in claim 13, wherein the step of decrypting said cipher-text

18 blocks includes employing said first pseudo random number, and/or said set of pair-wise

19 differentially-uniform pseudo random numbers.

Serial No.: 09/705,998

1   15. (Original) A method as recited in claim 13, wherein the step of combining includes:

2   pairing said first pseudo random number, and/or said set of pair-wise differentially-uniform

3   pseudo random numbers, with said plurality of plain-text blocks; and

4   using each pair to form a plurality of output blocks and employing the output blocks to form said

5   at least two check sums.

6   16. (Original) A method as recited in claim 15, wherein the step of using each pair includes

7   performing an exclusive-or operation upon components of said each pair.

8   17. (currently amended) A method as recited in claim 15, wherein the step of forming includes:

9   dividing the said output blocks into at least two subsets, and

10   obtaining said at least two checksums from an exclusive-or of said subsets of output blocks.

11   18. (Original) A method as recited in Claim 13, wherein the step of transforming said plain-text

12   blocks includes a non-cryptographic or linear operation.

13   19. (Original) A method as recited in Claim 13, wherein the step of transforming said plain-text

14   blocks includes a cryptographic operation.

15   20. (currently amended) A method as recited in Claim 13, wherein the said set of pair-wise

16   differentially-uniform numbers are set of pair-wise differentially-uniform numbers in GFp.

17   21. (Original) A method as recited in claim 14, wherein the step of employing includes:

DOCKET NUMBER: YOR920000763US1   **-8/34-**

PAGE 9/47 * RCVD AT 5/21/2004 2:13:07 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:9149453281 * DURATION (mm-ss):14-50

Serial No.: 09/705,998

1 pairing said first random number, and/or said first pseudo random number, and/or said set of

2 pair-wise differentially-uniform pseudo random numbers, with said plurality of cipher-text

3 blocks; and

4 combining each pair to form a plurality of input blocks used in said step of decrypting.

5 22. (Original) A method as recited in claim 3, wherein p is a prime number, and the step of

6 combining each pair includes performing a modulo p addition upon components of said each

7 pair.

8 23. (Original) A method as recited in claim 11, wherein p is a prime number, and the step of

9 combining each pair includes performing a modulo p addition upon components of said each

10 pair.

11 24. (Original) A method as recited in claim 15, wherein p is a prime number, and the step of

12 using each pair includes performing a modulo p addition upon components of said each pair.

13 25. (Original) A method as recited in claim 21, wherein p is a prime number, and the step of

14 combining each pair includes performing a modulo p addition upon components of said each

15 pair.

16 26. (Original) An article of manufacture comprising a computer usable medium having

17 computer readable program code means embodied therein for causing encryption of a plain-text

18 message, the computer readable program code means in said article of manufacture comprising

19 computer readable program code means for causing a computer to effect the steps of claim 1.

20 27. (Original) An article of manufacture comprising a computer usable medium having

21 computer readable program code means embodied therein for causing decryption of a cipher-text

22 message, the computer readable program code means in said article of manufacture comprising

23 computer readable program code means for causing a computer to effect the steps of claim 13.

DOCKET NUMBER: YOR920000763US1   **-9/34-**

PAGE 10/47 * RCVD AT 5/21/2004 2:13:07 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:9149453281 * DURATION (mm-ss):14-50

Serial No.: 09/705,998

1 28. (Original) A computer program product comprising a computer usable medium having

2 computer readable program code means embodied therein for causing encryption of a plain-text

3 message, the computer readable program code means in said computer program product

4 comprising computer readable program code means for causing a computer to effect the steps of

5 claim 1.

6 29. (Original) A computer program product comprising a computer usable medium having

7 computer readable program code means embodied therein for causing decryption of a plain-text

8 message, the computer readable program code means in said computer program product

9 comprising computer readable program code means for causing a computer to effect the steps of

10 claim 13.

11 30. (Original) A program storage device readable by machine, tangibly embodying a program of

12 instructions executable by the machine to perform method steps for encrypting a plain-text

13 message, said method steps comprising the steps of claim 1.

14 31. (Original) A program storage device readable by machine, tangibly embodying a program of

15 instructions executable by the machine to perform method steps for decrypting a cipher-text

16 message, said method steps comprising the steps of claim 13.

17 32. (Currently Amended) A method for encryption/decryption of a plain-text message, the

18 method comprising the steps of:

19 generating a first random number;

20 transforming said first random number into a first pseudo random number;

21 further expanding a randomness of said first random number and/or said first pseudo random

22 number into a set of pair-wise differentially-uniform pseudo random numbers;

Serial No.: 09/705,998

1   dividing the plain-text message into a plurality of plain-text blocks;

2   encrypting said plain-text blocks in forming a plurality of cipher-text blocks;

3   combining said plurality of plain-text blocks into at least one check sum; and

4   employing said first random number, said first pseudo random number and said set of pair-wise
5   differentially-uniform pseudo random numbers to embed a message integrity check in said
6   cipher-text blocks to form a cipher-text message; and

7   dividing said cipher-text message into a plurality of cipher-text blocks to form an encryption of
8   said plain-text message;

9   decrypting said cipher-text blocks in forming a plurality of plain-text blocks;

10   transforming at least one of said plain-text blocks into a first pseudo random number;

11   further expanding at least one of said plain-text blocks and/or said first pseudo random number
12   into a set of pair-wise differentially-uniform pseudo random numbers;

13   combining said first pseudo random number, and/or said set of pair-wise differentially-uniform
14   pseudo random numbers, and/or said at least one plain-text block to form at least two check sums
15   and to re-form the said plain-text message; and

16   comparing said at least two check sums in declaring success of a message integrity check in
17   decryption of said cipher-text to reform said plain-text message.

18   33. (Original) An apparatus to encrypt a plain-text message, the apparatus comprising:

DOCKET NUMBER: YOR920000763US1   -11/34-

PAGE 12/47 * RCVD AT 5/21/2004 2:13:07 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/1 * DNIS:8729306 * CSID:9149453281 * DURATION (mm-ss):14-50

Serial No.: 09/705,998

1   a Randomness Generator to generate a first random number;

2   a Randomness Transformer to transform said first random number into a first pseudo random

3   number;

4   a Pairwise Additively Uniform Sequence Generator to further expand a randomness of said first

5   random number and/or said first pseudo random number into a set of pair-wise

6   differentially-uniform pseudo random numbers;

7   an Encryptor to divide said plain-text message into a plurality of plain-text blocks, and to encrypt

8   said plain-text blocks to form a plurality of cipher-text blocks;

9   a Checksum Generator to combine said plurality of plain-text blocks into at least one check sum;

10   and

11   an Integrity Extractor and Checker to employ said set of pair-wise differentially-uniform pseudo

12   random numbers, together with said first random number and/or said first pseudo random

13   number, to embed a message integrity check in said cipher-text blocks.

14   34. (Original) An apparatus to decrypt a cipher-text message, the apparatus comprising:

15   a Decryptor to divide said cipher-text message into a plurality of cipher-text blocks, and to

16   decrypt said cipher-text blocks in forming a plurality of plain-text blocks;

17   a Randomness Transformer to transform at least one of said plain-text blocks into a first pseudo

18   random number;

19   a Pairwise Additively Uniform Sequence Generator to further expand at least one of said

20   plain-text blocks and/or said first pseudo random number into a set of pair-wise

21   differentially-uniform pseudo random numbers;

DOCKET NUMBER: YOR920000763US1   **-12/34-**

Serial N .: 09/705,998

1   a Checksum Generator to combine said first pseudo random number, and/or said set of pair-wise

2   differentially-uniform pseudo random numbers, and/or said at least one plain-text block to form

3   at least two check sums and to form a plurality of output blocks; and

4   an Integrity Extractor and Checker to compare said at least two check sums in declaring success

5   of a message integrity check.

6   35. (Original) An article of manufacture comprising a computer usable medium having

7   computer readable program code means embodied therein for causing encryption of a plain-text

8   message, the computer readable program code means in said article of manufacture comprising

9   computer readable program code means for causing a computer to effect the steps of claim 2.

10   36. (Original) An article of manufacture comprising a computer usable medium having

11   computer readable program code means embodied therein for causing decryption of a cipher-text

12   message, the computer readable program code means in said article of manufacture comprising

13   computer readable program code means for causing a computer to effect the steps of claim 14.

14   37. (Original) A computer program product comprising a computer usable medium having

15   computer readable program code means embodied therein for causing encryption of a plain-text

16   message, the computer readable program code means in said computer program product

17   comprising computer readable program code means for causing a computer to effect the steps of

18   claim 2.

19   38. (Original) A computer program product comprising a computer usable medium having

20   computer readable program code means embodied therein for causing decryption of a plain-text

21   message, the computer readable program code means in said computer program product

22   comprising computer readable program code means for causing a computer to effect the steps of

23   claim 14.

DOCKET NUMBER: YOR920000763US1   -13/34-

Serial No.: 09/705,998

1   39. (Original) A program storage device readable by machine, tangibly embodying a program of

2   instructions executable by the machine to perform method steps for encrypting a plain-text

3   message, said method steps comprising the steps of claim 2.

4   40. (Original) A program storage device readable by machine, tangibly embodying a program of

5   instructions executable by the machine to perform method steps for decrypting a cipher-text

6   message, said method steps comprising the steps of claim 14.

7   41. (Original) A method as recited in claim 3, wherein the step of combining each pair includes

8   performing an addition in a group upon components of said each pair.

9   42. (Currently Amended) A method as recited in claim 11, wherein the step of combining each

10   pair includes performing an addition in a group upon components of said each pair.

11   43. (Original) A method as recited in claim 15, wherein the step of using each pair includes

12   performing an addition in a group upon components of said each pair.

13   44. (Original) A method as recited in claim 21, wherein the step of combining each pair includes

14   performing an exclusive-or operation upon components of said each pair.

15   45. (Original) A method as recited in claim 21, wherein the step of combining each pair includes

16   performing an addition in a group upon components of said each pair.

17   46. (new) A method as recited in Claim 33, wherein at least one element performs a plurality of

18   operations in parallel.

19   47. (new) A method as recited in Claim 1, wherein the step of encrypting said plain-text blocks

20   is performed in parallel for a plurality of said plain-text blocks.